CIBERSEGURIDAD

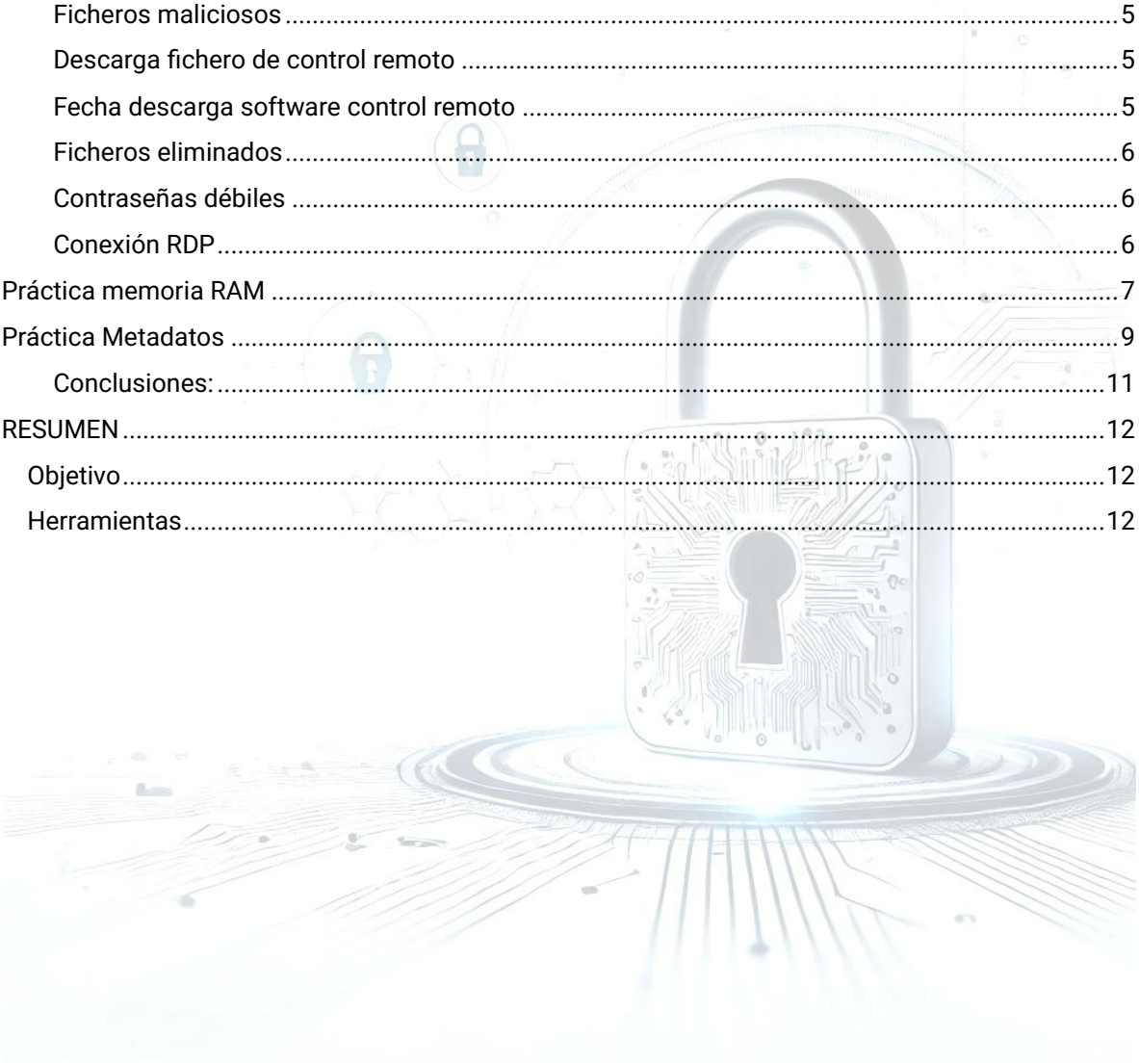
‘Bootcamp IX’

Informe Práctica Módulo DFIR.

Maximiliano Dariel Altamirano.

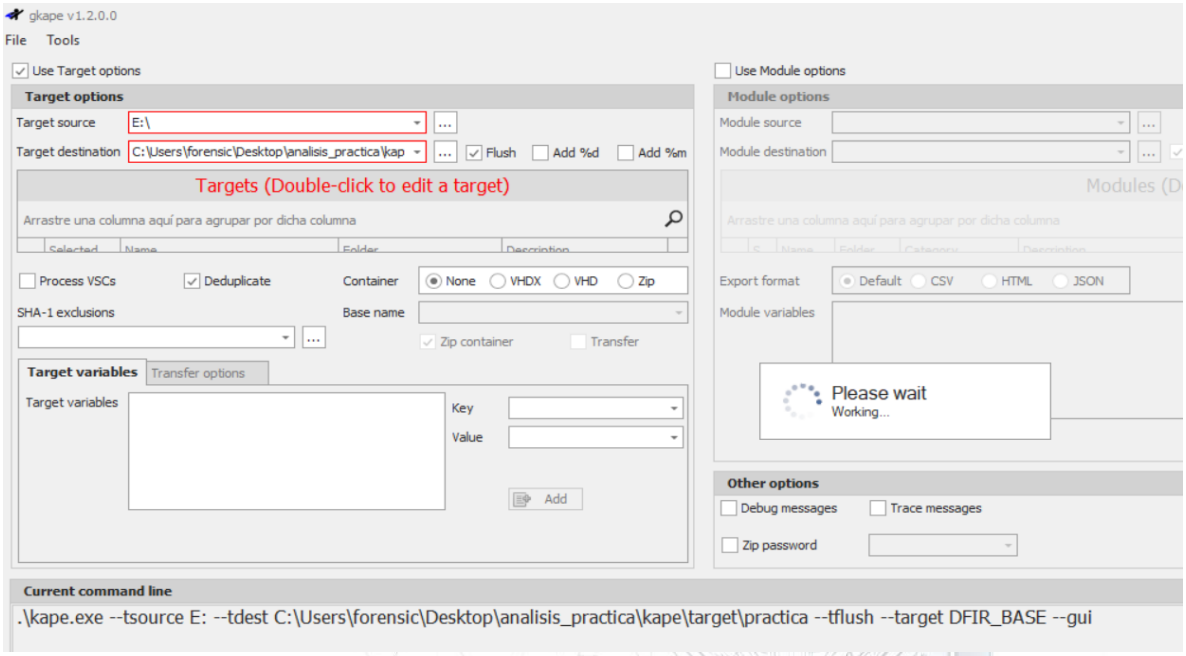
Academia KeepCoding.

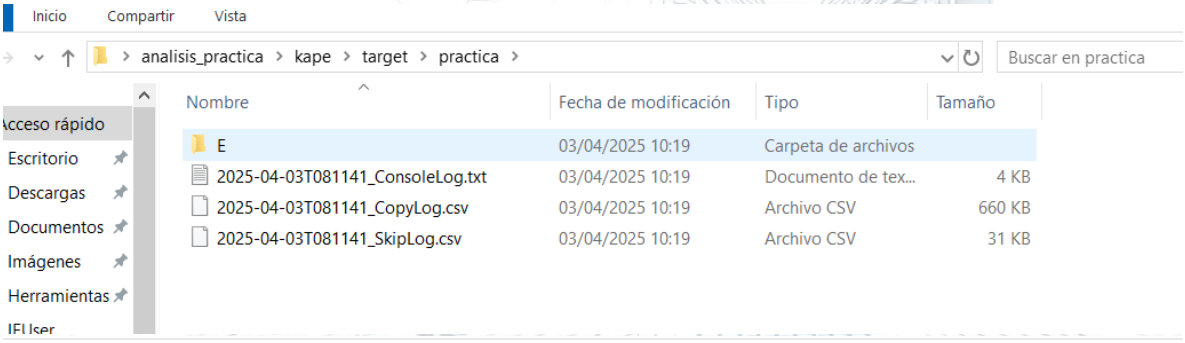
INDICE

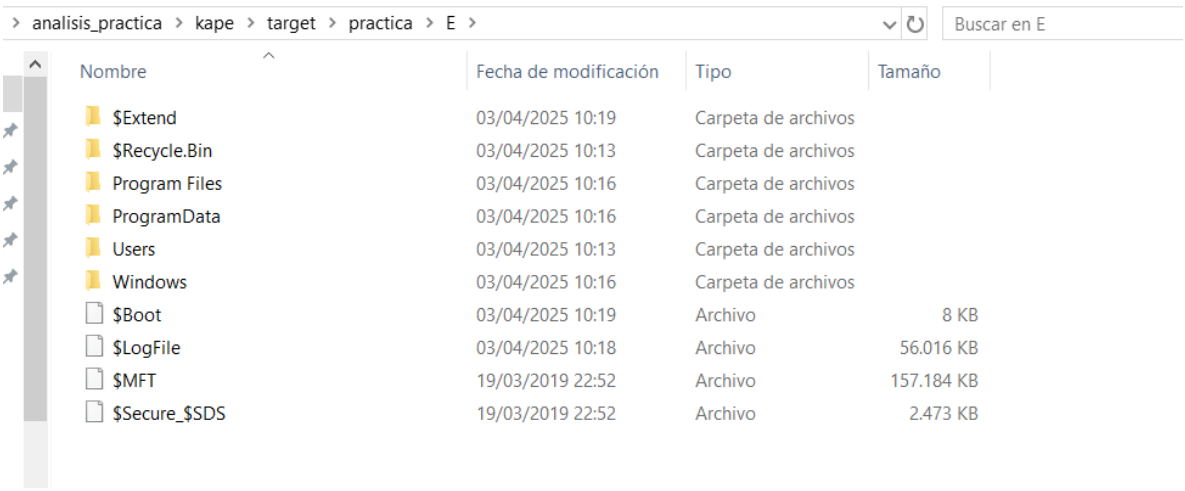


DESARROLLO

Para el análisis de la evidencia vamos a preprocesar los datos y ficheros con la herramienta Kape, utilizando el módulo target predefinido “DFIR_BASE.tkape”.







Práctica Windows

Avanzaremos en los desafíos propuestos en el enlace http://ctf.sancastell.me/challenges

Forensic

Hash del fichero

Valimos el hash del fichero con el siguiente comando en la consola de Windows

```
PS C:\Users\Usuario> Get-FileHash "C:\Users\Usuario\Downloads\Win10_PC001.vmdk" -Algorithm SHA256

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          4446E9C42345A32FA78A8CE20834FAA047A3B161EBA986F894D2230FCF6B0CBE       C:\Users\Usuario\Downloads\Wi...
```

Nombre de la máquina

Navegaremos las opciones con la herramienta RegistryExplorer para identificar el nombre de la máquina

Values

Arrastre una columna aquí para agrupar por dicha columna

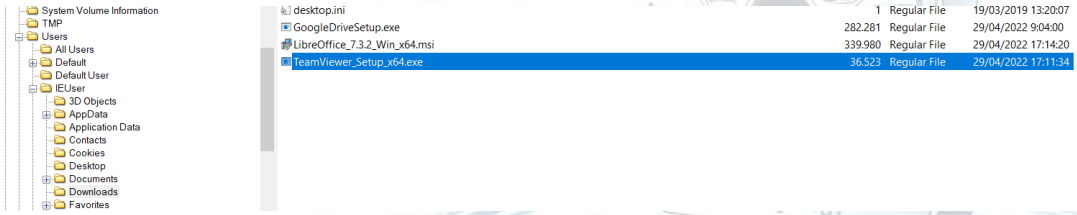
Value Name	Value Type	Data
(default)	RegSz	mnmsrvc
ComputerName	RegSz	PEGASUS01

Ficheros maliciosos

Utilizamos el módulo loki.exe para intentar identificar los ficheros maliciosos, obteniendo como ruta crítica E:\Users\Public

Descarga fichero de control remoto

Con la herramienta FTK Imager identificamos el archivo .exe de control remoto que ha descargado el usuario.



Fecha descarga software control remoto

Identificamos con la herramienta Timeline Explorer, procesando con Indx2Csv previamente el fichero $I30 del directorio Descargas del usuario, la fecha en la que hizo la descarga.

Seq No	File Name	CTime	ATime	RTime	MTime	Alloc S
	desktop.ini	2019-03-19 13:00:12.6307788	2019-03-19 13:20:07.9617970	2025-04-01 19:44:02.4318812	2025-04-01 19:47:30.1440619	288
	GoogleDriveSetup.exe	2022-04-29 09:03:30.3002502	2022-04-29 09:04:00.0315653	2022-05-08 18:57:28.2697323	2025-04-01 19:47:30.1440619	2890588
	GOOGLE~1.EXE	2022-04-29 09:03:30.3002502	2022-04-29 09:04:00.0315653	2022-05-08 18:57:28.2697323	2025-04-01 19:47:30.1440619	2890588
	LibreOffice_7.3.2_Win_x64.msi	2022-04-29 17:13:45.6342143	2022-04-29 17:14:20.9314537	2022-04-29 08:33:55.3434570	2025-04-01 19:47:30.1440619	3481395
	LIBREO~1.MSI	2022-04-29 17:13:45.6342143	2022-04-29 17:14:20.9314537	2022-04-29 08:33:55.3434570	2025-04-01 19:47:30.1440619	3481395
	TeamViewer_Setup_x64.exe	2022-04-29 17:11:25.0001198	2022-04-29 17:11:34.1956477	2022-04-29 09:20:32.2598800	2025-04-01 19:47:30.1440619	3740057
	TEAMVI~1.EXE	2022-04-29 17:11:25.0001198	2022-04-29 17:11:34.1956477	2022-04-29 09:20:32.2598800	2025-04-01 19:47:30.1440619	3740057

Ficheros eliminados

Con la herramienta UsnJrnl2Csv64.exe exploramos la información del fichero $J para identificar el fichero .zip eliminado

Contraseñas débiles

Para descubrir la contraseña, utilizamos el módulo mimikatz, lanzando el siguiente comando:

```
mimikatz # lsadump::sam /system:E:\Windows\System32\config\SYSTEM /sam:E:\Windows\System32\config\SAM
Domain : PEGASUS01
SysKey : ec022a77f903a7e69e603e0c84634ff0
```

Obteniendo como resultado el siguiente HASH

```
RID  : 000003e8 (1000)
User : IEUser
  Hash NTLM: 2d20d252a479f485cdf5e171d93985bf
```

Solo resta romper el hash desde https://crackstation.net/

QubesV3.1BackupDefaults

Hash	Type	Result
2d20d252a479f485cdf5e171d93985bf	NTLM	qwerty

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Conexión RDP

Hemos identificado el IP de conexión por RDP con los datos obtenidos desde los eventos de seguridad de Wind (192.168.183.134:445).

	PEGASUS01\IEUser	PEGASUS01 (-)	Target: PEGASUS01\Guest
credentials	PEGASUS01\IEUser	192.168.183.134:445	Target: PEGASUS01\user1
	WORKGROUP\PEGASUS01$	- (-)	Target: NT AUTHORITY\SYSTEM

Práctica memoria RAM

Haremos una adquisición desde nuestra RAM en Windows. Utilizaremos la herramienta *winpmem_mini_x64_rc2.exe*. Lanzaremos desde el CMD como administrador el siguiente comando:

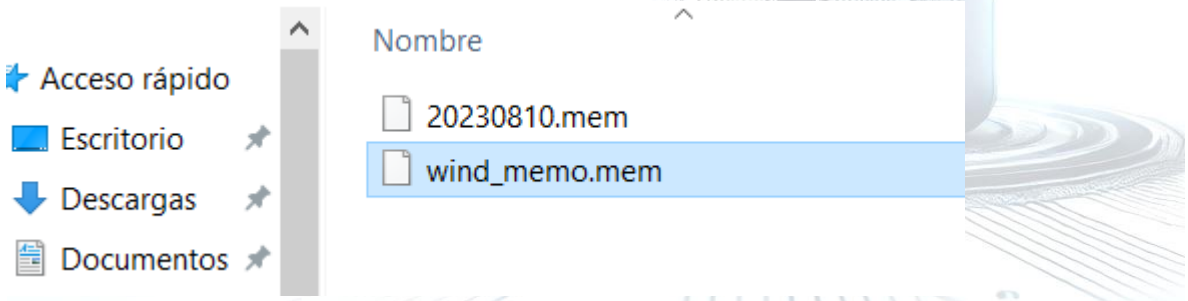
C:\Users\Usuario\Desktop\Formaciones>winpmem_mini_x64_rc2.exe C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem

```
Microsoft Windows [Versión 10.0.26100.3476]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>cd C:\Users\Usuario\Desktop\Formaciones

C:\Users\Usuario\Desktop\Formaciones>winpmem_mini_x64_rc2.exe C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem
WinPmem64
Extracting driver to C:\Users\Usuario\AppData\Local\Temp\pme1053.tmp
Driver Unloaded.
Loaded Driver C:\Users\Usuario\AppData\Local\Temp\pme1053.tmp.
Deleting C:\Users\Usuario\AppData\Local\Temp\pme1053.tmp
The system time is: 20:00:13
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AE000
 7 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x09900000
Start 0x09E00000 - Length 0x00100000
Start 0x09F0F000 - Length 0xAFA5A000
Start 0xBAB69000 - Length 0x0E216000
Start 0xCDFFF000 - Length 0x00001000
Start 0x100000000 - Length 0x40F340000
max_physical_memory_ 0x50f340000
Acquisition mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000
```

Generando el siguiente fichero(wind_memo.mem):



Utilizaremos *Volatility* para interpretar la memoria que hemos generado:

Lanzaremos los comandos más utilizados para el análisis (adquisición de RAM maquina Wind propia):

python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem windows.cmdline.CmdLine

```
C:\Users\Usuario\Desktop\Formaciones\volatility3-2.11.0\volatility3-2.11.0>python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem windows.cmdli
ne.CmdLine
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x20 is not valid (process exited?)
236     Secure System   Required memory at 0x20 is not valid (process exited?)
280     Registry        Required memory at 0x20 is not valid (process exited?)
796     smss.exe        Required memory at 0xce0c3d3020 is inaccessible (swapped)
1260    csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=bas
esrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
1404    wininit.exe     wininit.exe
1412    csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=bas
esrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
1504    winlogon.exe    winlogon.exe
1556    services.exe    C:\WINDOWS\system32\services.exe
1576    LsaIso.exe      Required memory at 0xe0e558c020 is inaccessible (swapped)
1584    lsass.exe       C:\WINDOWS\system32\lsass.exe
1720    svchost.exe     C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
1752    fontdrvhost.ex  Required memory at 0x1b070a17ab8 is inaccessible (swapped)
1760    fontdrvhost.ex
1852    svchost.exe     C:\WINDOWS\system32\svchost.exe -k RPCSS -p
1900    svchost.exe     C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p -s LSM
1988    dwm.exe "dwm.exe"
2028    svchost.exe     Required memory at 0x2db601050048 is inaccessible (swapped)
1552    svchost.exe     C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
1236    svchost.exe     Required memory at 0x1cb3e1050b8 is inaccessible (swapped)
1920    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService -p -s bthserv
1952    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService -p -s BthAvctpSvc
2096    svchost.exe     Required memory at 0x2cb45105048 is inaccessible (swapped)
2104    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
```

python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem windows.pslist.PsList

```
C:\Users\Usuario\Desktop\Formaciones\volatility3-2.11.0\volatility3-2.11.0>python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem windows.pslis
t.PsList
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x8d8a2c4b2040  349     -       N/A     False   2025-04-06 16:11:54.000000 UTC  N/A     Disabled
236     4       Secure System   0x8d8a2c6ec040  0       -       N/A     False   2025-04-06 16:11:52.000000 UTC  N/A     Disabled
280     4       Registry        0x8d8a2c7e6080  4       -       N/A     False   2025-04-06 16:11:52.000000 UTC  N/A     Disabled
796     4       smss.exe        0x8d8a3418b040  2       -       N/A     False   2025-04-06 16:11:54.000000 UTC  N/A     Disabled

Volatility experienced a symbol-related issue:
symbol_table_name1!_MM_SESSION_SPACE: Enumeration not found in symbol_table_name1 table: _MM_SESSION_SPACE

        * An invalid symbol table
        * A plugin requesting a bad symbol
        * A plugin requesting a symbol from the wrong table

No further results will be produced
```

python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem windows.pstree.PsTree

```
C:\Users\Usuario\Desktop\Formaciones\volatility3-2.11.0\volatility3-2.11.0>python vol.py -f C:\Users\Usuario\Desktop\Formaciones\wind_memo.mem windows.pstre
e.PsTree
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

4       0       System  0x8d8a2c4b2040  349     -       N/A     False   2025-04-06 16:11:54.000000 UTC  N/A     -       -       -
* 280   4       Registry        0x8d8a2c7e6080  4       -       N/A     False   2025-04-06 16:11:52.000000 UTC  N/A     Registry        -       -
* 236   4       Secure System   0x8d8a2c6ec040  0       -       N/A     False   2025-04-06 16:11:52.000000 UTC  N/A     -       -       -
* 796   4       smss.exe        0x8d8a3418b040  2       -       N/A     False   2025-04-06 16:11:54.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\Syst
em32\smss.exe   -       -
* 3932  4       MemCompression  0x8d8a3d0a7040  54      -       N/A     False   2025-04-06 16:12:05.000000 UTC  N/A     MemCompression  -       -

Volatility experienced a symbol-related issue:
symbol_table_name1!_MM_SESSION_SPACE: Enumeration not found in symbol_table_name1 table: _MM_SESSION_SPACE

        * An invalid symbol table
        * A plugin requesting a bad symbol
        * A plugin requesting a symbol from the wrong table

No further results will be produced
```

Práctica Metadatos

Analizaremos 3 imágenes incluidas en directorio *Imágenes (adjunta en la práctica)* con el módulo *exiftool*.

Para este punto enviaremos la imagen original tomada desde un terminal POCO F5 por dos medios, envío por Gmail y WhatsApp.

Para este punto evidenciamos el análisis de la imagen “original_1” del directorio “imagen_1”, obteniendo los siguientes resultados:

======== original_1.jpg	**======== gmail_1.jpg**	**======== wp_1.jfif**
ExifTool Version Number : 13.10	ExifTool Version Number : 13.10	ExifTool Version Number : 13.10
File Name : original_1.jpg	File Name : gmail_1.jpg	File Name : wp_1.jfif
Directory : .	Directory : .	Directory : .
File Size : 3.5 MB	File Size : 3.5 MB	File Size : 373 kB
File Modification Date/Time : 2025:04:06 00:02:04+02:00	File Modification Date/Time : 2025:04:06 00:02:04+02:00	File Modification Date/Time : 2025:04:06 00:02:05+02:00
File Access Date/Time : 2025:04:06 00:11:14+02:00	File Access Date/Time : 2025:04:06 00:11:14+02:00	File Access Date/Time : 2025:04:06 00:18:54+02:00
File Inode Change Date/Time : 2025:04:06 00:08:41+02:00	File Inode Change Date/Time : 2025:04:06 00:08:41+02:00	File Inode Change Date/Time : 2025:04:06 00:08:41+02:00
File Permissions : -rw-------	File Permissions : -rw-------	File Permissions : -rw-------
File Type : JPEG	File Type : JPEG	File Type : JPEG
File Type Extension : jpg	File Type Extension : jpg	File Type Extension : jpg
MIME Type : image/jpeg	MIME Type : image/jpeg	MIME Type : image/jpeg
Exif Byte Order : Big-endian (Motorola, MM)	Exif Byte Order : Big-endian (Motorola, MM)	JFIF Version : 1.01
Make : Xiaomi	Make : Xiaomi	Resolution Unit : None
Orientation : Horizontal (normal)	Orientation : Horizontal (normal)	X Resolution : 1
Modify Date : 2025:03:28 11:35:03	Modify Date : 2025:03:28 11:35:03	Y Resolution : 1
Y Resolution : 72	Y Resolution : 72	Image Width : 1640
X Resolution : 72	X Resolution : 72	Image Height : 1232
Camera Model Name : 23049PCD8G	Camera Model Name : 23049PCD8G	Encoding Process : Progressive DCT, Huffman coding
Y Cb Cr Positioning : Centered	Y Cb Cr Positioning : Centered	Bits Per Sample : 8
Exif Version : 0220	Exif Version : 0220	Color Components : 3
Aperture Value : 2.2	Aperture Value : 2.2	Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Scene Type : Directly photographed	Scene Type : Directly photographed	Image Size : 1640x1232
Mirror : false	Mirror : false	Megapixels : 2.0
Sensor Type : rear	Sensor Type : rear	
Hdr : auto	Hdr : auto	
Op Mode : 36869	Op Mode : 36869	
Small Picture : false	Small Picture : false	
AI Scene : 15	AI Scene : 15	
Filter Id : 66048	Filter Id : 66048	
Zoom Multiple : 0.6000000238418579	Zoom Multiple : 0.6000000238418579	

Exposure Compensation : 0	Exposure Compensation : 0	
Exposure Program : Program AE	Exposure Program : Program AE	
Color Space : sRGB	Color Space : sRGB	
Max Aperture Value : 2.2	Max Aperture Value : 2.2	
Exif Image Height : 2464	Exif Image Height : 2464	
Brightness Value : 7.92	Brightness Value : 7.92	
Date/Time Original : 2025:03:28 11:35:03	Date/Time Original : 2025:03:28 11:35:03	
Flashpix Version : 0100	Flashpix Version : 0100	
Sub Sec Time Original : 986	Sub Sec Time Original : 986	
White Balance : Auto	White Balance : Auto	
Interoperability Index : R98 - DCF basic file (sRGB)	Interoperability Index : R98 - DCF basic file (sRGB)	
Interoperability Version : 0100	Interoperability Version : 0100	
Exposure Mode : Auto	Exposure Mode : Auto	
Exposure Time : 1/753	Exposure Time : 1/753	
Offset Time : +01:00	Offset Time : +01:00	
Flash : Auto, Did not fire	Flash : Auto, Did not fire	
Sub Sec Time : 986	Sub Sec Time : 986	
F Number : 2.2	F Number : 2.2	
Exif Image Width : 3280	Exif Image Width : 3280	
ISO : 50	ISO : 50	
Components Configuration : Y, Cb, Cr, -	Components Configuration : Y, Cb, Cr, -	
Focal Length In 35mm Format : 16 mm	Focal Length In 35mm Format : 16 mm	
Sub Sec Time Digitized : 986	Sub Sec Time Digitized : 986	
Create Date : 2025:03:28 11:35:03	Create Date : 2025:03:28 11:35:03	
Shutter Speed Value : 1/753	Shutter Speed Value : 1/753	
Metering Mode : Center-weighted average	Metering Mode : Center-weighted average	
Focal Length : 1.6 mm	Focal Length : 1.6 mm	
Offset Time Original : +01:00	Offset Time Original : +01:00	
Scene Capture Type : Standard	Scene Capture Type : Standard	
Light Source : D65	Light Source : D65	
Sensing Method : Not defined	Sensing Method : Not defined	
Resolution Unit : inches	Resolution Unit : inches	
Xiaomi Model : POCO F5	Xiaomi Model : POCO F5	
Compression : JPEG (old-style)	Compression : JPEG (old-style)	
Thumbnail Offset : 10716	Thumbnail Offset : 10716	
Thumbnail Length : 25060	Thumbnail Length : 25060	
Image Width : 3280	Image Width : 3280	
Image Height : 2464	Image Height : 2464	
Encoding Process : Baseline DCT, Huffman coding	Encoding Process : Baseline DCT, Huffman coding	
Bits Per Sample : 8	Bits Per Sample : 8	
Color Components : 3	Color Components : 3	
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)	Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)	

Aperture : 2.2	Aperture : 2.2	
Image Size : 3280x2464	Image Size : 3280x2464	
Megapixels : 8.1	Megapixels : 8.1	
Scale Factor To 35 mm Equivalent: 9.7	Scale Factor To 35 mm Equivalent: 9.7	
Shutter Speed : 1/753	Shutter Speed : 1/753	
Create Date : 2025:03:28 11:35:03.986	Create Date : 2025:03:28 11:35:03.986	
Date/Time Original : 2025:03:28 11:35:03.986+01:00	Date/Time Original : 2025:03:28 11:35:03.986+01:00	
Modify Date : 2025:03:28 11:35:03.986+01:00	Modify Date : 2025:03:28 11:35:03.986+01:00	
Thumbnail Image : (Binary data 25060 bytes, use -b option to extract)	Thumbnail Image : (Binary data 25060 bytes, use -b option to extract)	
Circle Of Confusion : 0.003 mm	Circle Of Confusion : 0.003 mm	
Field Of View : 96.7 deg	Field Of View : 96.7 deg	
Focal Length : 1.6 mm (35 mm equivalent: 16.0 mm)	Focal Length : 1.6 mm (35 mm equivalent: 16.0 mm)	
Hyperfocal Distance : 0.40 m	Hyperfocal Distance : 0.40 m	
Light Value : 12.8	Light Value : 12.8	

Conclusiones:

Los metadatos originales se respetan en el envío por mail, pero no así en los servicios de mensajería (WhatsApp), ya que en este último perduran solo los indicadores “básicos” como metadatos.

Esto se debe a varios motivos:

Compresión: Algunas aplicaciones reduce el tamaño de las imágenes para ahorrar espacio, eliminando o modificando metadatos como la ubicación o los ajustes de la cámara. En nuestro análisis vemos reducido el tamaño del archivo y la calidad de la imagen en WhatsApp.

Privacidad: Algunas plataformas eliminan metadatos sensibles, como la geolocalización, para proteger la privacidad del usuario.

Optimización: Servicios como Gmail pueden ajustar el formato o la resolución de las imágenes para facilitar su envío y visualización.

Dejamos evidencia en el mismo directorio de 2 imágenes más con resultados similares a este.

RESUMEN

Objetivo

El informe pretende dejar en evidencia las herramientas y conocimientos adquiridos en el módulo DFIR, explorando desde una máquina virtual, todas las herramientas revisadas en clases.

Herramientas

Para el avance de utilizamos las siguientes herramientas:

- Virtual Box – Windows 10
- Virtual Box - Kali